RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Babel Revisited: Lessons from an IPv6 Transition

SESSION ID: TECH-R04A

Jeffrey J. Wiley
Sr. Advisor to CISO
Internal Revenue Service
@wiley_jay

Steven F. Fox
Sr. Security Architecture and Engineering Advisor
Internal Revenue Service
@securelexicon

If as one people speaking the same language they have begun to do this, then nothing they plan to do will be impossible for them.

Genesis 11:7

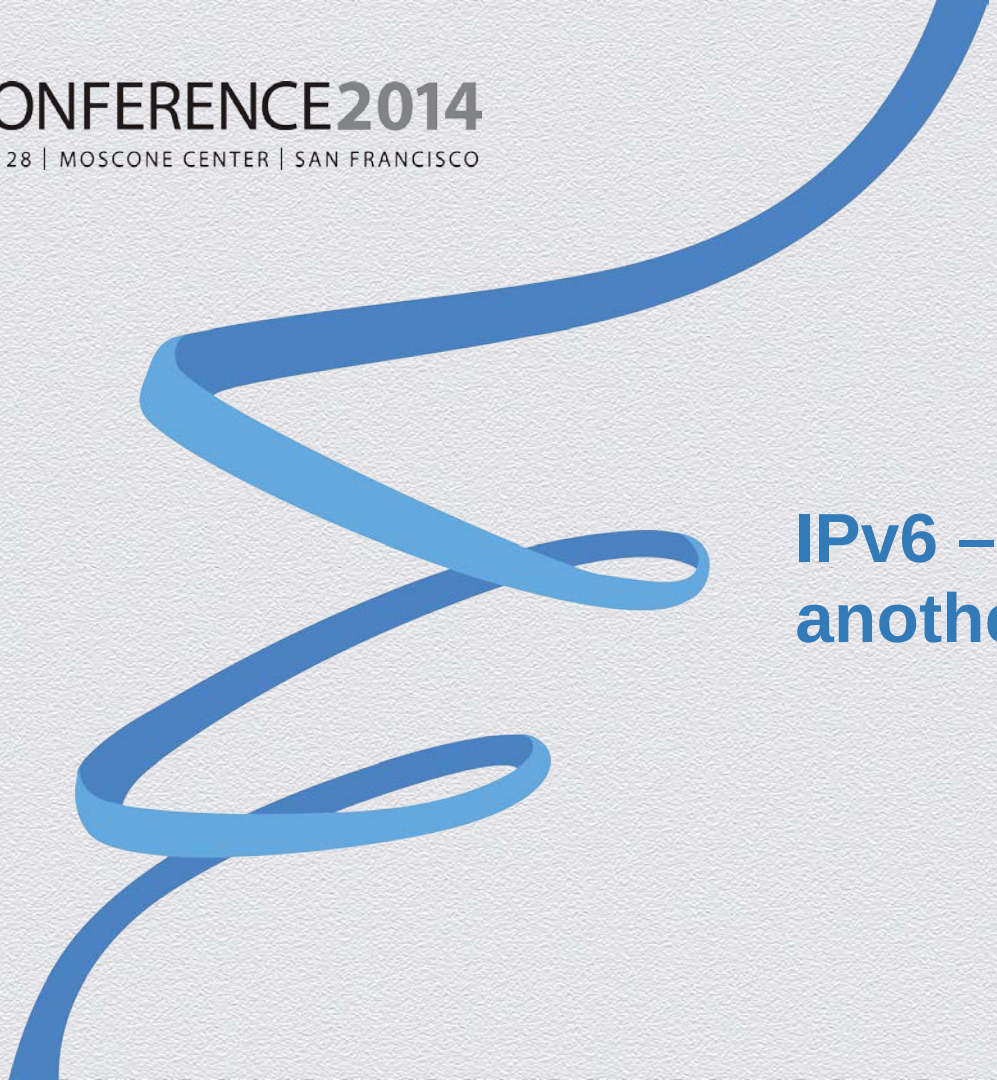
#RSAC
RSACONFERENCE2014

Agenda

- Introduction
- Why we invested in IPv6
- Challenges we encountered
- Our team-based approach
- Plans for the future
- Take-aways

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



IPv6 – Not just another upgrade

IPv6

- New network functionality
- Routing improvements
- Built-in authentication and privacy support
- Improvement to IP administration

IRS

#RSAC

RSACONFERENCE2014

Why transition to IPv6?

IPv6 Drivers for Government

OMB Mandate - 2012

External Facing

- Internet
- E-Mail
- ISP Services

OMB Mandate - 2014

Upgrade client applications

- Communicate with public Internet servers
- Communicate with supporting enterprise networks

IRS

IRS Transition Drivers

- IRS Mission Drivers
  - Portal upgrade
  - Windows 7 upgrade
  - Computer Center consolidation
- Federal Acquisition Regulations

#RSAC
RSACONFERENCE2014

1. Document external-facing assets
2. Document intranet assets

Transition risks informed by technology and governance baselines.

#RSAC
RSACONFERENCE2014

Transition Challenges

Strategy

Procurement

Vendor Readiness

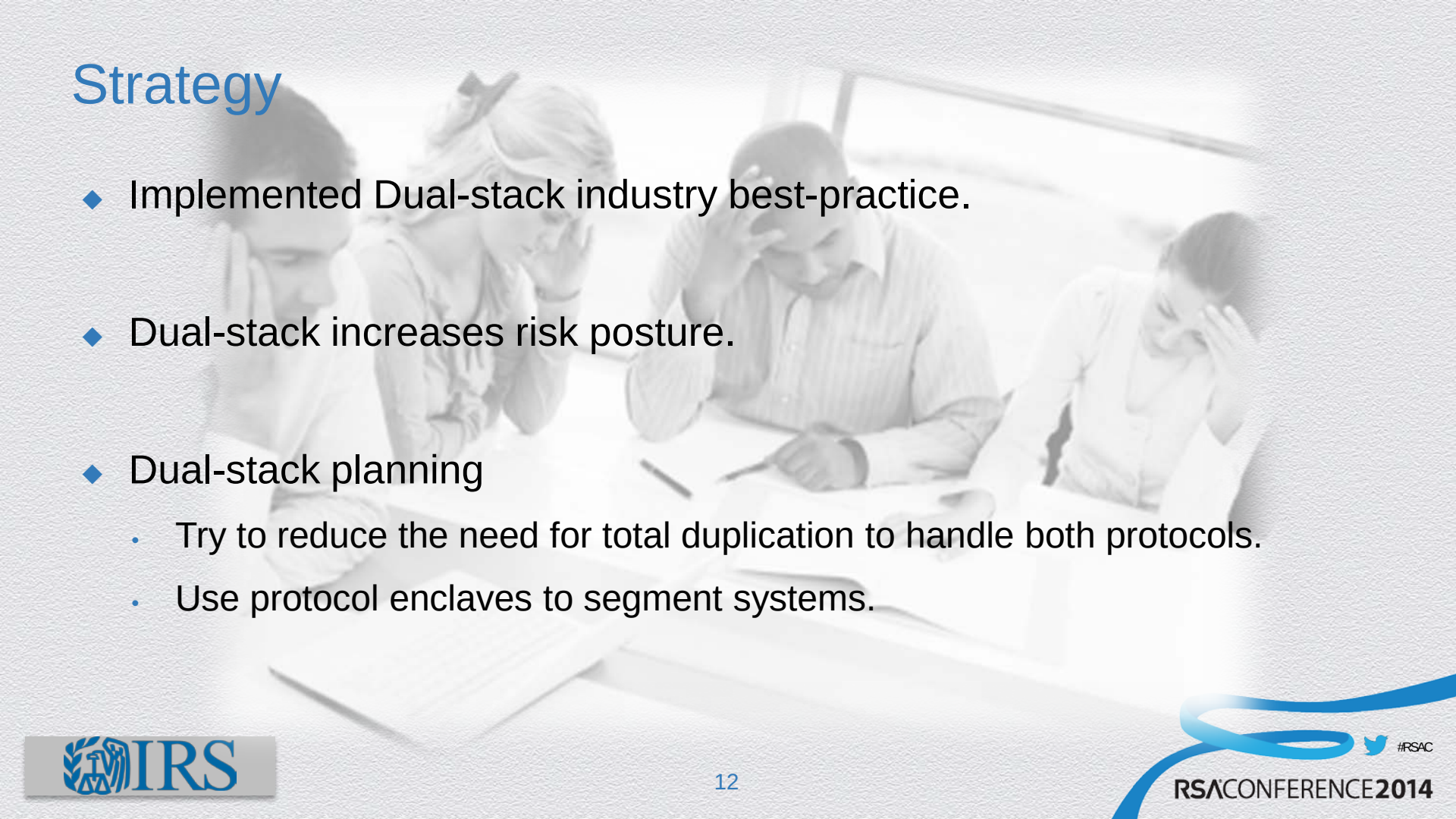
Security Architecture

#RSAC
RSACONFERENCE2014

Strategy

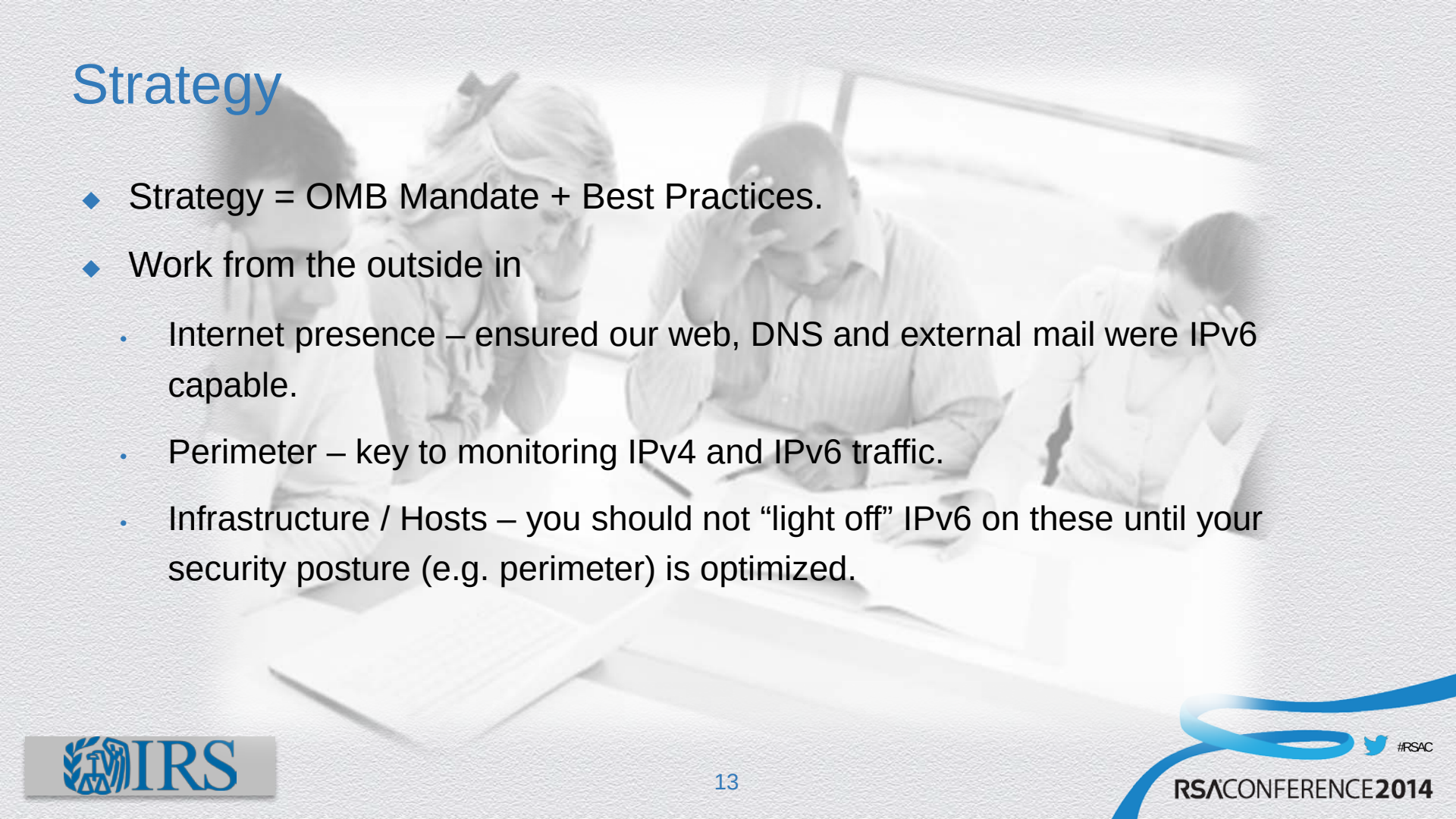
- Challenge was adapting to the new protocol.
  - Increased risk
  - Policy
  - WAN limitations
- Perimeter re-design to accommodate technology insertion.

Strategy



- Implemented Dual-stack industry best-practice.
- Dual-stack increases risk posture.
- Dual-stack planning
  - Try to reduce the need for total duplication to handle both protocols.
  - Use protocol enclaves to segment systems.

Strategy



- Strategy = OMB Mandate + Best Practices.
- Work from the outside in
  - Internet presence – ensured our web, DNS and external mail were IPv6 capable.
  - Perimeter – key to monitoring IPv4 and IPv6 traffic.
  - Infrastructure / Hosts – you should not “light off” IPv6 on these until your security posture (e.g. perimeter) is optimized.

Procurement Readiness

- Mid-point product rollout revealed procurement issues
  - Procurement did not account for IPv6 requirements.
  - Policy to procure only IPv6-capable products in place for over 4 years!
- This led to a change in the procurement contracts
  - Add boiler plate language to all affected contracts

#RSAC
RSACONFERENCE2014

Procurement Readiness

Procurement did not account for IPv6 requirements

- On one level, there were instances of products in procurement that simply were not IPv6-ready.

- One level deeper, there was an instance of a product having IPv6 capabilities insufficient to perform to the same level as in our IPv4 domain.

Procurement Readiness

Policy to procure only IPv6-capable products in place for over 4 years!

- Contract language was reviewed and changed much too late.
- When is the time you should engage Supply Chain to make these adjustments?
- This can be a land mine for your teams

#RSAC
RSACONFERENCE2014

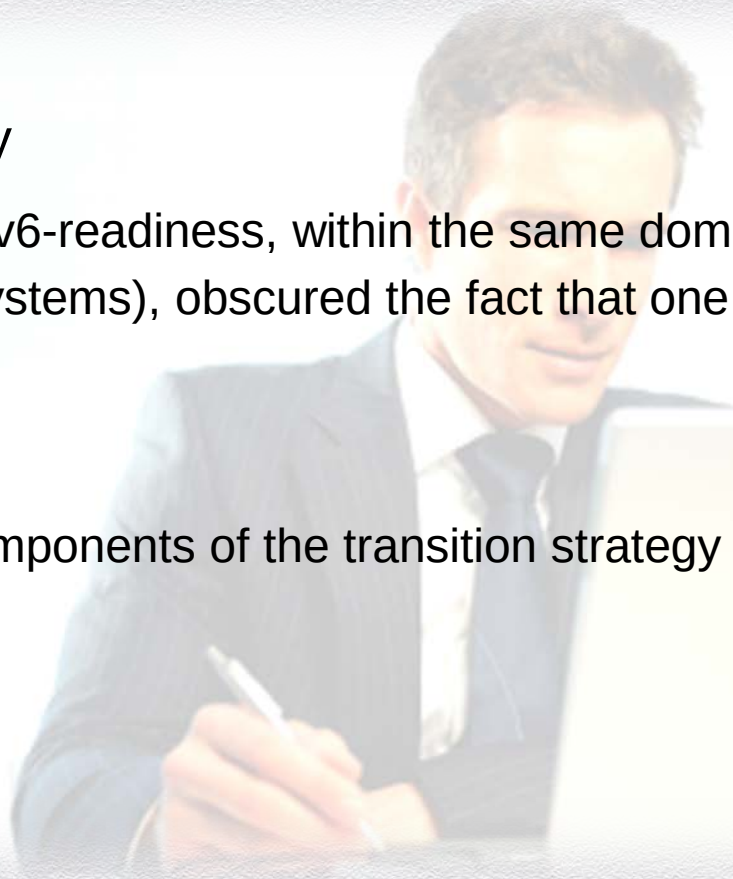
Vendor Readiness

- Major vendor not IPv6 compliant
  - Discovered this well into the transition.
  - No vendor roadmap on these platforms.

- Impact on network and security architecture influenced transition strategy.

#RSAC
RSACONFERENCE2014

Vendor Readiness



Major vendor not IPv6-ready

- Multiple vendors meeting IPv6-readiness, within the same domain (e.g. Host-based Intrusion Detection systems), obscured the fact that one major vendor was not IPv6-ready.

- Architecture and vendor components of the transition strategy updated.

Security Architecture

- Challenge was to adapt to a new protocol.

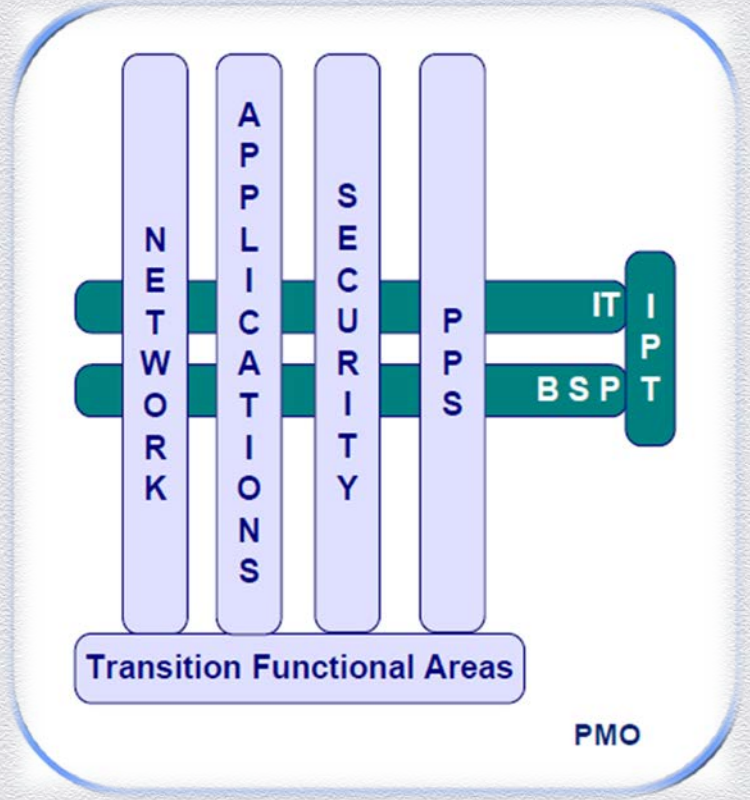
- Security architecture modified to:
  - Respond to vendor and procurement challenges.
  - Handle our transition mechanism.
  - Maintain security capability.

Security Architecture

- Made several changes to our internal architecture to accommodate and respond to the aforementioned vendor and procurement challenges.
- Absolute requirement to maintain your capabilities (e.g. deep-packet inspection) in the IPv6 domain.
- We also ensured the security architecture could handle our transition mechanism. We discuss that next.

Transition success requires a team!

Transition team



#RSAC
RSACONFERENCE2014

Governance

- Policy
- Requirements
- Standards

Network

- Network infrastructure
- Tackled procurement and vendor management challenges.

Application

Managed IPv6 readiness gap for software

- IRS-developed
- COTS

Security

Security assurance

- Policy
- Engineering
- Technical Operations
- Accreditation
- Executive Oversight

Security Requirements Development

IPv6 Security Requirements – Authoritative Sources

- Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government (Federal CIO Council)
- Guideline for the Secure Deployment of IPv6 (NIST SP 800-119)
  - All RFCs listed within (numerous)
- USGv6 Profile and Testing Program (NIST SP 500-267)
- U.S. Federal Acquisition Regulation (FAR)
- Locator / Identifier Separation Protocol (IETF RFC 6830)
- IPv6 Security (Hogg and Vyncke, ciscopress.com, 2009)

Plans for the future

Future work

- IPv6 Pilot
- Verification and Validation
- Testing
- Locator / Identifier Separation Protocol (LISP)

Take-aways for next week.

Vendor Readiness

- Use IPv6 test labs.
- IPv4 enclave work-around.

Procurement

- Negotiate expedited version release.
- Create policy enclaves.

Security Architecture

- Position NIDS within the perimeter.
- Monitor data on tunnel egress point.

Strategy

- Dual-stack using LISP – RFC 6830.

#RSAC
RSACONFERENCE2014

Action items

- Build a transition team.
- Identify procurement needs and *change* policies in advance.
- Verify vendor capabilities through test labs (here are two):
  - https://www.iol.unh.edu/services/testing/ipv6/
  - https://www.icsalabs.com/technology-program/ipv6
- Promote transition efforts throughout the organization.
- Use authoritative sources as foundation for security / operational requirements.
- Remember our challenges and lessons learned.

Meet us for Hallway Q/A

#RSAC
RSACONFERENCE2014